**IT Applications, Unit 4**

**Ch 8, Security and Ethical Considerations**

**Disaster Recovery Strategies, p 514**

1. What is a disaster recovery plan?

* A disaster recovery plan is a document that tells an organisation what steps are needed to restore the company operations, including computing in the event of a disaster.

Preparing a disaster recovery plan:

* Conduct a risk assessment
* Identify recovery strategies and procedures
* Purchase products and services to support disaster recovery
* Test the system and maintain a plan

1. List some considerations required in preparing a disaster recovery plan.

* Store passwords in to separate secure locations, one of which is in the same building; the second location might be offsite
* Document the whole recovery process including the location of systems recovery disks. Make sure that all key staff members are familiar with the disaster recovery plan
* Establish an automated system to notify key staff members of a failure in the system. These staff members should be able to know how to start implementing the disaster recovery plan
* Practice the disaster recovery plan on a quarterly basis. Ensue that new staff understand the process and that all staff are kept up to date with new equipment or software
* Make sure that your backup system works and occurs regularly
* Build redundancy into your system to eliminate as many points of failure as possible
* Ensure that you have replacement equipment
* As part of the archive strategy, replace tapes used for backup every 6-9 months
* Buy the best UPS that you can afford
* Protect yourself from theft and employee malice. Ensure data server room is always locked
* Automatically closing fire doors will keep fire and smoke out of the room

There are four key parts to a disaster recovery plan:

1. Preparing an emergency plan

* An emergency plan explains specific steps to be taken in the event of a natural disaster
  1. What should an emergency plan contain?
  + Names and contact details of people to notify including management and emergency services
  + Procedures to follow with the computer equipment such as equipment shutdown or removal of files
  + Evacuation procedures for employees including removal of backup tapes or equipment
  + Return procedures detailing who may re-enter the facility and under what circumstances
  + Details of equipment suppliers are insurance providers so that the information system can be rebuild as quickly as possible `

1. Preparing a “backup” plan
   1. What does a backup plan involve?
   * A backup plan covers the procedures that the company is to follow for using file backups to restore computer systems
   1. List what the plan should include
   * The location of alternative sites and equipment in case the normal computer facility has been destroyed
   * The location of backup data, supplies and equipment
   * The personnel responsible for gathering backup resources and transporting them to alternative computing facility
   * A schedule indicating the other and approximate time in which each application should be up and running
2. Preparing a recovery plan
   1. What does a recovery plan involved?

A recovery plan includes specific procedures for restoring the full information processing capacity of the organisation.

* 1. What are the things to consider when writing a recovery plan?
  + Identification of mission critical ICT services; these will have first priority when getting the system back online
  + Use of a backup (or secondary) site for data processing needs until the primary site has been removed

1. Test plan
   1. What is looked for in testing a disaster recovery strategy?

Points of weakness that will prevent the various emergency, backup and recovery plans from working seamlessly

**Evaluating information-management strategies,** p 517

Elaborate on each of the following four criteria to consider in evaluating information-management strategies:

1. Integrity of data

Data integrity depends on its accuracy, reliability and timeliness. Whether storing, transmitting or archiving data, you must be sure that its integrity is maintained. Otherwise that data may not be accessible when needed.

1. Security

If you have spent a great deal of money securing your data from threats, you want to be sure that the data security is effective. Audit trains and log files can alert you to any problems within logon or file access procedures.

1. Ease of retrieval

Proper observance of folder and file naming conventions will help staff to find documents. If the conventions are difficult to follow files may be ‘lost’ or they may take more time to find. Using correct file extensions is important because it allows recognition by application software.

1. Currency of files

Regular backups will help to ensure that the mist recent versions of files are available if needed. If there has been a disaster and backup files are needed to restore the system, determine how much data has actually been lost whether or not this is within the amount of tolerated by the organisation.